HHS Enterprise Information Security Policy (EIS-Policy)

Version 2.0

Revised

November 14, 2016

TABLE OF CONTENTS

Security Policy Document Statement

The HHS Enterprise Information Security Policy (EIS-Policy) provides a framework for the protection of HHS information resources. The security objectives of confidentiality, integrity and availability (CIA) are best achieved through the implementation of these policies.

HHS management, which includes Enterprise and agency management, is responsible for the review, approval and enforcement of this Enterprise Information Security Policy.

For purpose of this EIS-Policy, the term “HHS management” refers specifically to individual HHS agency officials empowered with the authority and accountability to ensure implementation of the EIS-Policy. For the purpose of the security program the word “Enterprise” is synonymous with “system.”

The Office of the Chief Information Security Officer is the issuing authority for the Enterprise Information Security Policy (EIS-Policy).

Revisions

Date of Revision	Revision made by	Title	Version	Summary of Revision
6/30/2014	Khatija S Syeda Glen Boyer Frederick A Lawson	Project Manager, HHS Office of CISO TIERS Component ISSO Information Security Analyst HHS Office of CISO	1.0	Initial document authored.
8/5/2015	Khatija S Syeda	Deputy Information Security Officer HHSC	1.1	Annual review of the HHS EIS-Policy. Revised the Data Classification Policy. Added the Information Security Program Framework. Added the responsibilities for information custodian from TAC 202 (Definitions).
8/11/15	Khatija S Syeda	Deputy Information Security Officer HHSC	1.1	Final
6/28/16	Shirley Erp Sridhar Kosaraju	CISO App Sec Lead	2.0	Annual review of the HHS EIS-Policy. Included Secure-SDLC, mobile, risk assessments for external entities, cloud, secure remote computing, and program name change to "system"; updated based on MARS-E 2.0
11/14/16	Steven P. Pryor	Information Security Analyst HHSC	2.0	Final

Reviews

To satisfy the requirements of the Information Security Program, a formal review of this document is mandatory whenever significant changes occur in the environment.

Reviewer	Job Title	Review Date
Shirley Erp	HHS Chief Information Security Officer (CISO)	7/5/14
Anita Strayer	HHSC Information Security Officer (ISO)	7/8/14
Shenny Sheth	DADS Information Security Officer (ISO)	7/20/14
Matt Riemersma	DARS Information Security Officer (ISO)	7/14/14
Mark Herber	DFPS Information Security Officer (ISO)	7/18/14
Kevin White	DSHS Information Security Officer (ISO)	7/21/14
Kim Wendland	Enterprise Customer Services and Support	8/27/14
Laura Leigh Wolbrueck	HHSC IT Business Services	8/28/14
Paul Diaz	HHSC IT Operations	9/2/14
Agency IRMs approved		9/4/14

Reviewer	Job Title	Review Date
Shirley Erp	HHS Chief Information Security Officer (CISO)	8/6/2015
Glen Boyer	HHSC Information Security Officer (ISO)	8/5/2015

Reviewer	Job Title	Review Date
Shirley Erp	HHS Chief Information Security Officer (CISO)	8/4/2016
Stan Hogan	HHSC Information Security Officer (ISO)	8/4/2016
Mark Herber	DFPS Information Security Officer (ISO)	8/4/2016
Kevin White	DSHS Information Security Officer (ISO)	8/4/2016
John Makamson	TIERS Information System Security Officer (ISSO)	8/4/2016
Cynthia Dollar	Legal	8/4/2016

1. PURPOSE

Title 1, Texas Administrative Code (TAC), Chapter 202, RULE §202.24 Agency Information Security Program requires that all state agencies have an information security program consistent with the rules defined in the TAC 202. The Texas Health and Human Services (HHS) Circular C-021, HHS Enterprise Information Security Policy (EIS-Policy) and the Enterprise Information Security Standards and Guidelines (EISSG) Controls Catalog establishes the HHS system Information Security Program for the Health and Human Services System and is consistent with Title 1 TAC 202 rules.

The HHS system Information Security Program (SIS-Program) establishes the information security criteria for information and information systems that support the operations and assets of the organization, including contractors.
The primary goal of Information Security is to protect the confidentiality, integrity, and availability of information and information resources. Security policies, standards, controls, guidelines, procedures, and practices provide the document structure for communicating security objectives throughout the HHS Enterprise. Content contained in each of these documents will be as follows:

- **Policy** – consists of **high-level strategic statements** relating to the protection of confidentiality, integrity, and availability of information resources across the organization.

- **Standards** – consists of a set of **rules on a topic that are tactical, measurable, and specific** and may contain a subset of security controls for enforcing or support information security policy.

- **Controls** – consists of **specific technical and management safeguards for information systems** that are selected and must be met in accordance with defined security requirements.

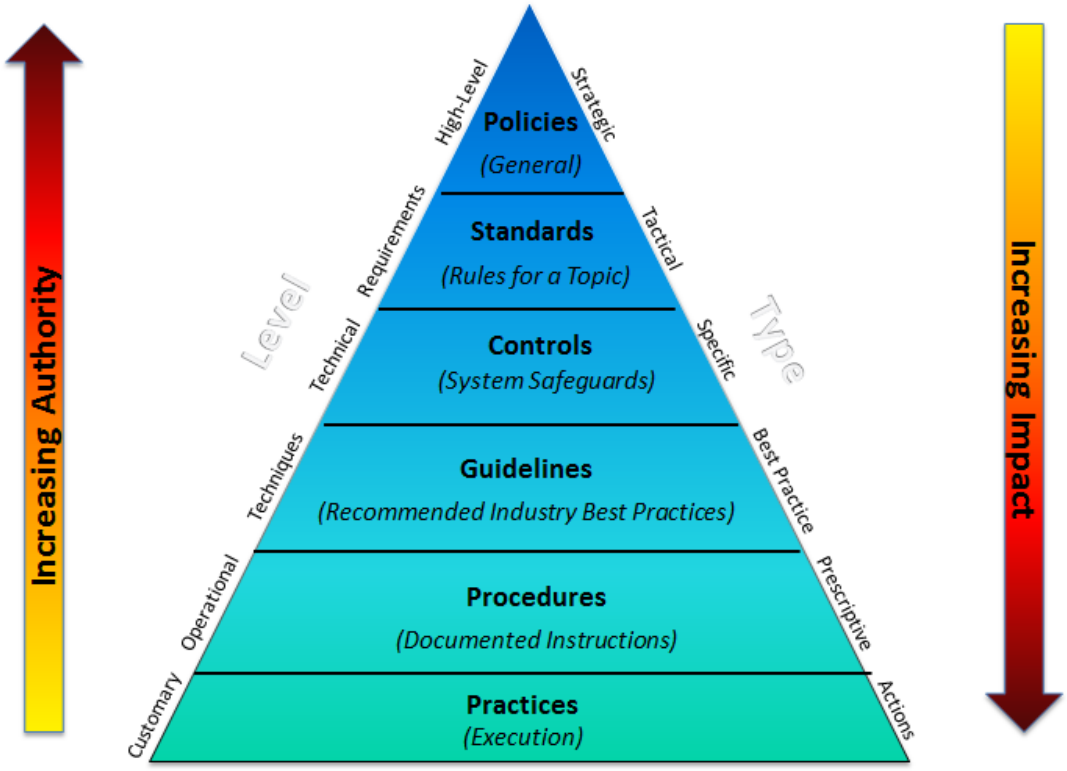
- **Guidelines** – consists of **recommended industry best practice techniques** that help support standards or serve as a reference when no applicable standard is in place.

- **Procedures** – consists of **documented operational instructions** that may prescribe a process or contain a series of steps for assisting workers with implementing security requirements.

- **Practices** – consists of **executed customary actions** that may not be documented.

The following diagram illustrates the relationship within these SIS-Program document types and where the EISSG Controls Catalog fits into the overall SIS-Program.

HHS Enterprise Information Security Framework



HHS management is committed to the protection of information and computing assets within the HHS environment (physical surroundings in which an information system processes, stores and transmits information), the fulfillment of the RULE §202.24 Agency Information Security Program requirement, and the HHS Circular C-021. To that end, HHS management has enabled a comprehensive information security program across HHS through the development, publication, monitoring, review, and enforcement of the baseline information systems security policies (hereafter referred to as the "Enterprise Information Security Policy" also referred to as EIS-Policy contained within this document.

This security policy incorporates the requirements of federal, state, and agency regulations as listed in Section 9 (Laws, Regulations & Guidance).

HHS EIS-Policy establishes a set of comprehensive policies that regulate access to HHS information systems within the HHS environment (internal and external) and the information processed, stored, and transmitted by them.

2. SCOPE

HHS policies apply to all HHS employees, contractors and third party users of HHS information resources. These policies also apply to all HHS information systems, IT activities, and IT assets that are owned, leased, or controlled, including mobile and other assets that may be used for HHS purposes. In addition, these policies apply to information assets, whether standalone or attached to the HHS local and wide area networks, that store, process or transmit HHS electronic data, as well as, all services that support or otherwise handle HHS information assets including outsourced resources to another agency, contractor, third party entities, cloud computing or other sources.

The EIS-Policy does not apply to clients or customers of HHS services.

Each HHS agency must determine their information system categorization level by evaluating the potential impact value (high, moderate, low), and associate the security level to each of the three security objectives of confidentiality, integrity, and availability (CIA). This process leads to a security categorization which forms the basis for selecting appropriate security controls for assessing system risk.

Applying appropriate policies, measures, and priorities for HHS information systems involves the concept of determining/utilizing security objectives, impact levels and security categorization. Each is described below.

Security objectives of confidentiality, integrity, and availability (CIA) are:

- Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability - Ensuring timely and reliable access to and use of information.

Impact levels are defined as follows:

- The potential impact is low if the loss of CIA could be expected to have a limited adverse effect on the organization's operations, assets, or individuals;
- The potential impact is moderate if the loss of CIA could be expected to have a serious adverse effect on the organization's operations, assets, or individuals;
- The potential impact is high if the loss of CIA could be expected to have a severe or catastrophic adverse effect on the organization's operations, assets, or individuals.

With the determination of impacts for each security objective, an appropriate security category of high, medium or low is obtained. Risks to information resources shall be managed. The expense of security safeguards shall be commensurate with the value of the assets being protected.

The management of risk is a key element in HHS's information security program and provides an effective framework for selecting appropriate security controls necessary to protect HHS information assets. HHS policy statements and associated policy procedures were developed for a "moderate" impact category system and form the baseline for assessment, analysis, and management of HHS IT risk. However, a portion of the information systems are "low" impact category system and those systems would require a lesser/reduced set of controls. HHS's information security program has

developed a set of “tailored” controls for low impact categorization systems; please refer to the HHS Enterprise Information Security Standards and Guidelines (EISSG) for those tailored controls.

3. ROLES AND RESPONSIBILITIES

Regardless of position or job classification, every employee and contractor that works in the HHS environment (physical surroundings in which an information system processes, stores, and transmits information) plays an important role in safeguarding the confidentiality, integrity, and availability of the systems and the data maintained by HHS. It is important that each individual fully understands his or her role and its associated responsibilities as designated by the HHS information security program and abides by the security policies, security controls, and procedures set forth by the HHS CISO.

Role	Responsibility
HHS Chief Information Security Officer (CISO)	An individual directed by the HHS Executive Commissioner or his/her designee to develop and maintain the HHS system Information Security Program. The CISO is responsible to: a) Provide leadership, direction, and coordination for the HHS system Information Security Program. b) Maintain the HHS system Information Security Program, which is a risk-based and collaborative effort among the HHS agency ISOs and other stakeholders. c) Explore, recommend, and implement system security strategies, tools, and resources for HHS efficiencies. d) Monitor and report on the compliance and effectiveness of system security strategies. e) Establish an Information Security Associate (ISA) program for communicating, training, and delegating security responsibilities throughout the system. f) Develop and implement a comprehensive system-wide training and awareness program.
Agency Information Security Officer (ISO)	An individual directed by the HHS Executive Commissioner or his/her designee to report to the HHS system CISO and also have a formal relationship with their respective agency's executive management. The Agency ISO is responsible for the specifics of their agency's security program, and are responsible to: a) Keep the CISO informed on agency information security related issues, events, and incidents. b) Communicate their agency's information security needs to the CISO. c) Collaborate on, provide input to, and actively participate in the SIS Program.

Role	Responsibility
	d) Administer the system and agency information security programs. e) Implement procedures and practices aligned with the SIS Program to ensure the security of information resources. f) Establish procedures for assessing and ensuring compliance with information security policies through inspections, reviews, and evaluations. g) Establish an agency Information Security Training and Awareness Program, which compliments the system initiatives. h) Develop and maintain an agency-wide information security plan as required by Government Code §2054.133. i) Work with the business and technical resources to ensure that security controls are utilized to address all applicable requirements. j) Provide guidance and assistance to senior agency officials, information owners, information custodians, and end users concerning their responsibilities. k) Ensure that annual information security risk assessments are performed and documented by information owners. l) Review and update annually the agency's inventory of information systems and related ownership and responsibilities. m) Review and update or respond to the data security requirements, specifications and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential information. n) Verify that appropriate security requirements are in place for the purchase of required information technology hardware, software, and systems development services for any new mission critical computer applications or computer applications that receive, maintain, and/or share confidential information. o) Monitor the compliance and effectiveness of defined security controls.
Information Owner	An individual with statutory or operational authority for specified information or information resources. The owner or his/ her designated representative(s) are responsible for:

Role	Responsibility
	a) Classifying information under their authority, with the concurrence of the HHS agency head or his/ her designated representative(s), in accordance with agency's established information classification categories. b) Approving access to information resources and periodically reviewing access lists based on documented risk management decisions. c) Formally assigning custody of information or an information resource. d) Coordinating data security control requirements with the ISO. e) Conveying data security control requirements to custodians. f) Providing authority to custodians to implement security controls and procedures. g) Justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the agency information security officer; and h) Participating in risk assessments.
Information Custodian	A department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource and are responsible for: a) Implementing controls required to protect information and information resources based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the agency information security program. b) Providing owners with information to evaluate the cost-effectiveness of controls and monitoring. c) Adhering to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents; d) Providing information necessary for appropriate information security training to employees; and e) Ensuring information is recoverable in accordance with risk management decisions;

Role	Responsibility
	f) Implementing an audit record review strategy that establishes the type of event that occurred and the identity of the individual associated with the event.
Application, Server, Database, Network Administrators	Verifies that server, database, and network security requirements (as described in the Enterprise Information Security Standards and Guidelines and as defined in the information system security plan) are being met: a) Establishes and communicates the security safeguards required for protecting server, database, and network security based on the sensitivity levels of the information. b) Periodically reviews and verifies that all users of their servers, databases, and network resources are: • authorized • use the required systems security safeguards • in compliance with the policies contained within this document and all related security controls and procedure requirements.
System Developers	Ensures that HHS information security requirements (as described in the Enterprise Information Security Standards and Guidelines and as defined in the information system security plan) are being met: a) Develops and implements the HHS information security requirements throughout the System Development Life Cycle (SDLC). Also known as Secure-SDLC (S-SDLC). b) Plans and implements for the on-going maintenance of the information system, including updates, upgrades, and patches in accordance with the S-SDLC and security policies within this document.
Service Providers, Vendors, and Contractor Employees	Ensures the protection of HHS information (data) and information systems by: a) Complying with the information security requirements maintained in this policy. b) Complying with the individual HHS agency information policy requirements.
Users	An individual, a process, or an automated application authorized to access an information resource in accordance

Role	Responsibility
	with federal and state law, agency policy, and the information owner's procedures and rules. The user of an information resource has the responsibility to: a) Use the resource only for the purpose specified by the agency or information owner. b) Comply with information security controls and agency policies to prevent unauthorized or accidental disclosure, modification, or destruction; and c) Formally acknowledge that they will comply with the security policies and procedures in a method determined by the agency head or his/her designated representative.
Others	Other roles and responsibilities as required by HHS agreements or contracts.

4. IMPLEMENTATION

The procedures to facilitate the implementation of the HHS information security policies contained in this document consist of:

- Publish the HHS information security policies on the HHSC Intranet site.
- The EIS-Policy will utilize the HHS Enterprise Information Security Standards and Guidelines (EISSG) that establishes the minimum security controls for HHS to support federal and state requirements and to ensure protection of information resources from unlawful or unauthorized access, use, modification or destruction or disclosure.
- An assessment of the security controls using the EISSG shall be performed to assure that they have been implemented correctly and are working effectively in support and enforcement of these information security policies.
- While there is a requirement for all policies to be implemented, there shall be a risk-based, phased approach for the implementation of these policies and the expense and strength of security safeguards shall be commensurate with the value of the assets being protected.
- Additional procedures that support the implementation of these policies shall also be on a risk-based, phased approach.
    - The controls to facilitate the implementation of the HHS Information Security policies are located at HHS Enterprise Information Security Standards and Guidelines (EISSG). http://hhscx.hhsc.texas.gov/it/policies-and-guidelines

5. MANAGEMENT COMMITMENT

HHS management recognizes the role of information security in ensuring that users have access to the information they require in order to carry out their work. Any reduction in the CIA of information could prevent HHS from functioning effectively and efficiently. In addition, the loss or unauthorized disclosure of information has the potential to damage the reputation of HHS and cause financial loss.

HHS agency IT divisions and business areas that manage IT resources or oversee contractors that maintain HHS confidential information are responsible to assess security risks for their confidential data or systems, and/or for their contractors, and take appropriate actions to mitigate any identified risks. This includes locations maintained internally by an HHS agency, a contractor, or by a different HHS agency. Assessments should consider IT resources located in areas that are publicly accessible. Restricted area entry and exit points shall be secured to assure appropriate access to information resources.

To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard-copy form. HHS management is committed to protecting the security of its information and information systems in order to ensure that:

- The missions of the agencies are supported.
- Confidentiality is not breached so that information is accessed only by those authorized to do so.
- Ensuring timely availability and reliable access to information resources.
- The integrity of information is maintained so that it is accurate and up to date.
- HHS meets its federal, state and legal requirements.
- The reputation of HHS is safeguarded.

The HHS Enterprise Information Security Policy protects not only information and systems, but also individual employees and HHS as a whole. As such, these policies represent HHS management's strong commitment to information systems security.

6. COORDINATION

Representatives from all relevant parts of the HHS organization shall coordinate the implementation of the information security policies.

HHS agencies may make further policy additions which cannot contradict or weaken the HHS Enterprise Information Security Policy.

HHS management will establish and maintain appropriate contacts with HHS organizational entities, other organizations, law enforcement authorities, regulatory bodies, and network and telecommunications operators with respect to information security policy.

Users of HHS information will be made aware of their own individual responsibilities for complying with HHS policies on information security.

7. REVIEW AND EVALUATION

The HHS Office of the Chief Information Security Officer in collaboration with the HHS agencies' Information Security Officers (ISO's) shall develop, disseminate, review, and update this security policy as significant changes occur in the environment.

8. COMPLIANCE

Compliance with the EIS-Policy is mandatory. Reviews shall be conducted to assure compliance is undertaken at established intervals using authorized methods.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment (for full time and temporary employees); a termination of employment relations (in the case of contractors or consultants); dismissal (for interns and volunteers). Additionally, individuals are subject to loss of HHS information resources access privileges, and to civil and criminal prosecution.

9. LAWS, REGULATIONS & GUIDANCE

Federal, state, and agency regulations, along with guidance in the form of HHS policies and standards, are mandatory and are critical drivers for the HHS Information Security Program. Compliance with these regulations is required, based upon the mission of each agency. The HHS Enterprise Information Security policies do not replace, but are in addition to these requirements.

Listed below are the federal, state and agency regulations that define the requirements for data handling and information system security that the HHS Information Security Program and the Enterprise Information Security policies are based upon:

Federal

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- The Health Information Technology for Economic and Clinical Health (HITECH) Act, ARRA Components, 2009
- Internal Revenue Service Publication 1075, Tax Information Security Guidelines for federal, state, and local agencies and entities

- Center for Medicaid & Medicare Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- Criminal Justice Information Services (CJIS)
- Social Security Administration (SSA) Guidelines
- Family Educational Rights and Privacy Act (FERPA)

State

- Title 1, Part 10 Texas Administrative Code, Chapter 202: Information Security Standards
- Texas Business and Commerce Code

Agency

- HHS Circular C-021 HHS Enterprise Information Security Policy
- HHS Enterprise Information Security Standards and Guidelines (EISSG)

10. ENTERPRISE INFORMATION SECURITY POLICIES

Information security policies are high level statements of HHS goals and objectives for the protection of information resources. An information security policy is the documentation of enterprise-wide decisions on handling and protecting information resources.

Policy statements are more specific statements of management intent such as "HHS management is responsible for ensuring that limited access to applications, servers, databases and network devices occur within the HHS environment." Policy statements are made up of statements for ensuring the confidentiality, integrity, and availability (CIA) of information resources that exist within the HHS environment.

10.1 Data Classification Policy (DCP)

The Data Classification Policy provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by federal and state law as well as proprietary, operational, and privacy considerations. All HHS data, whether electronic or printed, shall be classified. Consistent use of data classification reinforces with users the expected level of protection of HHS data assets in accordance with HHS security policies.

The HHS Data Classification Policy applies equally to all individuals who use or handle any HHS information resource. Data shall be classified in accordance with the table below.

HHS data created, sent, printed, received, or stored on systems owned, leased, administered, or authorized by the HHS agencies is the property of the HHS agency and its protection is the responsibility of the HHS owners, designated custodians, and users.

Data shall be classified as follows from highest level of sensitivity to the lowest:

Table 10.1	
Confidential	***Summary :*** • Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement. Information that is exempt from the Texas Public Information Act. ***Details:*** "**Confidential Information"** means any communication or record (whether oral, written, electronically stored or transmitted, or in any other form) provided to or made available to CONTRACTOR or that CONTRACTOR may create, receive, maintain, use, disclose or have access to on behalf of HHS that consists of or includes any or all of the following: (1) Client Information; (2) Protected Health Information in any form including without limitation, Electronic Protected Health Information or Unsecured Protected Health Information; (3) Sensitive Personal Information defined by Texas Business and Commerce Code Ch. 521; (4) Federal Tax Information; (5) Personally Identifiable Information; (6) Social Security Administration Data, including, without limitation, Medicaid information; (7) All privileged work product;

	(8) All information designated as confidential under the constitution and laws of the State of Texas and of the United States, including the Texas Health & Safety Code and the Texas Public Information Act, Texas Government Code, Chapter 552.
Agency Sensitive	• Agency sensitive information is information that is not subject to specific legal, regulatory or other external requirements, but is considered HHS sensitive and should not be readily available to the public. Agency sensitive information must be protected even though disclosure is not specifically restricted by legal or regulatory requirements.
Public	• Information that is freely and without reservation made available to the public. • Information intended or required for public release as described in the Texas Public Information Act. (https://www.tsl.texas.gov/agency/customer/pia.html)

More detailed information on data classification is located in the HHS Data Classification Standard.

10.2 Access Control Policy (AC)

HHS management is responsible for ensuring that limited access to information resources occurs within the HHS environment. Information resources assigned from one state agency to another or from a state agency to a contractor or other third party, at a minimum, shall be protected in accordance with the conditions imposed by the providing state agency.

Access Control Policy Statements

The following access control policy statements are required to satisfy the access control policy.

10.2.1 **Account Management:** HHS management shall ensure that all accounts accessing HHS information resources are managed. **(EISSG Control Reference: AC-2)**

10.2.2 **Access Enforcement:** HHS management shall enforce approved authorizations for logical access to HHS information resources. **(EISSG Control Reference: AC-3)**

10.2.3 **Information Flow Enforcement:** HHS management shall enforce approved authorizations for controlling the flow of information within the HHS components and between interconnected systems. **(EISSG Control Reference: AC-4)**

10.2.4 **Separation of Duties:** HHS management shall ensure that a separation of duties exists between distinct information system support functions to prevent malevolent activity without collusion. **(EISSG Control Reference: AC-5)**

10.2.5 **Least Privilege:** HHS management shall ensure that the concept of least privilege is employed, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned tasks. **(EISSG Control Reference: AC-6)**

10.2.6 **Unsuccessful Logon Attempts:** HHS management shall enforce a limit on unsuccessful logon attempts by users of HHS information resources. **(EISSG Control Reference: AC-7)**

10.2.7 System Use Notification: HHS management shall ensure that an approved system use notification or banner is displayed before granting access to HHS information resources. **(EISSG Control Reference: AC-8)**

10.2.8 Concurrent Session Control: HHS management shall employ a limit on the number of concurrent sessions for each system account to one (1). **(EISSG Control Reference: AC-10)**

10.2.9 Session Lock: HHS management shall employ session lock mechanisms after a period of inactivity has occurred to prevent further access to the system. **(EISSG Control Reference: AC-11)**

10.2.10 Session Termination: HHS management shall ensure the information system terminates a user session at the end of the session or when it has reached the limit of inactivity permitted. **(EISSG Control Reference: AC-12)**

10.2.11 Permitted Actions without Identification or Authentication: HHS management shall identify specific user actions that can be performed on HHS information systems without identification or authentication. **(EISSG Control Reference: AC-14)**

10.2.12 Remote Access: HHS management shall document and manage methods of secure remote access to HHS information resources. **(EISSG Control Reference: AC-17)**

10.2.13 Wireless Access: HHS management shall ensure the management of wireless usage and restrictions for access to HHS information resources. **(EISSG Control Reference: AC-18)**

10.2.14 Access Control for Mobile Devices: HHS management shall ensure the management of mobile device access to HHS information resources. **(EISSG Control Reference: AC-19)**

10.2.15 Use of External Information Systems: HHS management shall establish terms and conditions consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems including cloud-based systems and services. **(EISSG Control Reference: AC-20)**

10.2.16 Information Sharing: HHS management shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information. **(EISSG Control Reference: AC-21)**

10.2.17 Publicly Accessible Content: HHS management shall ensure the management of publicly accessible content for HHS. **(EISSG Control Reference: AC-22)**

10.3 Security Awareness and Training Policy (AT)

HHS management is responsible for ensuring that users, including contractors of the HHS information system, are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, guidelines, and procedures related to the security of the HHS information system.

Security Awareness and Training Policy Statements

The following security awareness and training policy statements are required to satisfy the security awareness and training policy.

10.3.1 Security Awareness Training Policy and Procedures: HHS management shall develop, disseminate, review and update a formal documented security awareness and training policy and document procedures to facilitate the implementation. (EISSG Control Reference: AT-1)

10.3.2 Security Awareness Training: HHS management shall ensure that HHS users receive basic security awareness training provided by HHS. **(EISSG Control Reference: AT-2)**

10.3.3 Role-Based Security Training: HHS management shall ensure that role-based security training is provided. **(EISSG Control Reference: AT-3)**

10.3.4 Security Training Records: HHS management shall ensure that a process exists to document and manage an individual's security training activities. **(EISSG Control Reference: AT-4)**

10.4 Audit and Accountability Policy (AU)

HHS management is responsible for ensuring the creation, protection, and retention of HHS audit records.

Audit and Accountability Policy Statements

The following audit and accountability policy statements are required to satisfy the audit and accountability policy.

10.4.1 Audit Events: HHS management shall require identification and listing of significant auditable security events. **(EISSG Control Reference: AU-2)**

10.4.2 Content of Audit Records: HHS management shall require HHS information systems to be able to produce audit records that contain sufficient information. **(EISSG Control Reference: AU-3)**

10.4.3 Audit Storage Capacity: HHS management shall require adequate storage capacity be allocated for audit log needs. **(EISSG Control Reference: AU-4)**

10.4.4 Response to Audit Processing Failures: HHS management shall ensure that appropriate mechanisms are in place to respond to audit failures or audit storage capacity issues. **(EISSG Control Reference: AU-5)**

10.4.5 Audit Review, Analysis and Reporting: HHS management shall require a review and analysis of HHS audit records on a periodic basis for indications of inappropriate or unusual activity, and report findings to designated HHS officials. **(EISSG Control Reference: AU-6)**

10.4.6 Audit Reduction and Report Generation: HHS management shall ensure that HHS information systems provide audit reduction and report generation capability. **(EISSG Control Reference: AU-7)**

10.4.7 Time Stamps: HHS management shall ensure that HHS information systems use internal system clocks to generate time stamps for audit records and the system clocks shall be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). **(EISSG Control Reference: AU-8)**

10.4.8 Protection of Audit Information: HHS management shall ensure that HHS information systems protect audit information and audit tools from unauthorized access, modification, and deletion. **(EISSG Control Reference: AU-9)**

10.4.9 Non-Repudiation: HHS management shall ensure that HHS information systems protect against an individual falsely denying having performed a particular action. **(EISSG Control Reference: AU-10)**

10.4.10 Audit Record Retention: HHS management shall ensure that HHS information systems retain audit records and archive old records to provide support for investigations and to meet regulatory requirements**. (EISSG Control Reference: AU-11)**

10.4.11 Audit Generation: HHS management shall ensure that HHS information systems provide audit record generation capability for the list of auditable events. **(EISSG Control Reference: AU-12)**

10.4.12 Cross-Organizational Auditing: HHS management shall ensure that HHS systems preserve the identity of individuals across organizational boundaries. **(EISSG Control Reference: AU-16)**

10.5 Security Assessment and Authorization Policy (CA)

HHS management shall ensure that (i) an initial assessment of the security controls for key information systems is performed to determine if the controls are effective in their application; (ii) controls are monitored on an ongoing basis to ensure their continued effectiveness; (iii) information systems containing potential vulnerabilities due to deficiencies in their controls are documented and acknowledged by the HHS management or his/ her designee and (iv) plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities are developed and implemented.

Security Assessment and Authorization Policy Statements

The following security assessment and authorization policy statements are required to satisfy the security assessment and authorization policy.

10.5.1 Security Assessments: HHS management shall ensure that the security controls identified in the HHS System Security Plan are assessed on a periodic basis. **(EISSG Control Reference: CA-2)**

10.5.2 System Interconnections: HHS management shall require the use of interconnection security agreements for connections to information systems outside of the HHS authorization boundary. **(EISSG Control Reference: CA-3)**

10.5.3 Plan of Action and Milestones: HHS management shall require the development and submittal of a plan of action and milestones (POA&M) to document any planned remedial actions to correct security deficiencies. **(EISSG Control Reference: CA-5)**

10.5.4 Security Authorization: HHS management shall ensure that HHS is assigned a senior level executive or manager as the HHS authorizing official. **(EISSG Control Reference: CA-6)**

10.5.5 Continuous Monitoring: HHS management shall ensure a continuous monitoring strategy is implemented as part of the HHS Information Security Program. **(EISSG Control Reference: CA-7)**

10.5.6 Internal System Connections: HHS management shall ensure all internal connections to the information system shall be authorized. **(EISSG Control Reference: CA-9)**

10.6 Configuration Management Policy (CM)

HHS management shall (i) establish and maintain baseline configurations and inventories of HHS information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in HHS information systems.

Configuration Management Policy Statements

The following configuration management policy statements are required to satisfy the configuration management policy.

10.6.1 **Configuration Management Policy and Procedures:** HHS management shall ensure the development, documentation and dissemination of procedures to applicable personnel. **(EISSG Control Reference: CM-1)**

10.6.2 **Baseline Configuration:** HHS management shall develop, document, and maintain under configuration control, a current baseline configuration of the HHS information system and its components. **(EISSG Control Reference: CM-2)**

10.6.3 **Configuration Change Control:** HHS management shall ensure the management of configuration change control for HHS through the Change Control Board (CCB). Configuration change management shall include determining the types of changes that are controlled, approving and documenting configuration-controlled changes, retaining and reviewing records of configuration-controlled changes, and coordinating and providing oversight for configuration change control activities. **(EISSG Control Reference: CM-3)**

10.6.4 **Security Impact Analysis:** HHS management shall analyze changes to HHS information resources to determine potential security impacts prior to change implementation. **(EISSG Control Reference: CM-4)**

10.6.5 **Access Restrictions for Change:** HHS management shall ensure physical and logical access restrictions associated with changes to HHS information resources are defined, documented, approved and enforced. **(EISSG Control Reference: CM-5)**

10.6.6 **Configuration Settings:** HHS management shall establish, document, and implement mandatory configuration settings for information technology products employed within HHS. HHS management shall manage exceptions and monitor changes to the configuration settings. **(EISSG Control Reference: CM-6)**

10.6.7 **Least Functionality:** HHS management shall ensure the configuration of HHS information systems to provide only essential capabilities and specifically prohibit or restrict the use of certain resources (functions, ports, protocols, and/or services). **(EISSG Control Reference: CM-7)**

10.6.8 **Information System Component Inventory:** HHS management shall develop, document, and maintain an information system component inventory for HHS. **(EISSG Control Reference: CM-8)**

10.6.9 **Configuration Management Plan:** HHS management shall develop, document, and implement a configuration management plan for HHS. **(EISSG Control Reference: CM-9)**

10.6.10 Software Usage Restrictions: HHS management shall ensure the use of software and associated documentation in accordance with contract agreements and copyright laws. **(EISSG Control Reference: CM-10)**

10.6.11 User-Installed Software: HHS management shall establish standards and guidelines governing the installation of software by users. **(EISSG Control Reference: CM-11)**

10.7 Contingency Planning Policy (CP)

HHS management shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for HHS information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Contingency Planning Policy Statements

The following contingency planning policy statements are required to satisfy the contingency planning policy.

10.7.1 Contingency Plan: HHS management shall develop a contingency plan (CP) for HHS. **(EISSG Control Reference: CP-2)**

10.7.2 Contingency Training: HHS management shall train operational and support personnel (including managers and users of HHS information resources) in their contingency roles and responsibilities. **(EISSG Control Reference: CP-3)**

10.7.3 Contingency Plan Testing: HHS management shall test the contingency plan for HHS. **(EISSG Control Reference: CP-4)**

10.7.4 Alternate Storage Site: HHS management shall establish an alternate storage site to permit the storage and recovery of HHS backup information. **(EISSG Control Reference: CP-6)**

10.7.5 Alternate Processing Site: HHS management shall establish an alternate processing site to permit the resumption of HHS operations for essential missions and business functions. **(EISSG Control Reference: CP-7)**

10.7.6 Telecommunications Services: HHS management shall establish alternate telecommunications services to permit the resumption of HHS operations for essential missions and business functions. **(EISSG Control Reference: CP-8)**

10.7.7 Information System Backup: HHS management shall ensure that user-level and system-level information as well as documentation of the systems are backed up. HHS management shall protect the confidentiality, integrity and availability of backup information at the storage location. **(EISSG Control Reference: CP-9)**

10.7.8 Information System Recovery and Reconstitution: HHS management shall provide for the recovery and reconstitution of HHS information system to a known state after a disruption, compromise, or failure. **(EISSG Control Reference: CP-10)**

10.8 Identification and Authentication Policy (IA)

HHS management shall ensure the identification of information system users, processes acting on behalf of users, or devices and authenticates (or verifies) the identities of those users, processes, or devices as a prerequisite to allowing access to HHS information resources.

Identification and Authentication Policy Statements

The following identification and authentication policy statements are required to satisfy the identification and authentication policy.

10.8.1 **Identification and Authentication (Organizational Users):** HHS information systems shall uniquely identify and authenticate HHS users (or processes acting on behalf of users). **(EISSG Control Reference: IA-2)**

10.8.2 **Device Identification and Authentication:** HHS information systems shall uniquely identify and authenticate specific and/or types of devices before establishing a connection. **(EISSG Control Reference: IA-3)**

10.8.3 **Identifier Management:** HHS management shall manage information system identifiers for users and devices. **(EISSG Control Reference: IA-4)**

10.8.4 **Authenticator Management:** HHS management shall manage component authenticators for users and devices. **(EISSG Control Reference: IA-5)**

10.8.5 **Authenticator Feedback:** HHS information systems shall obscure feedback of authentication information during the authentication process to protect the information from unauthorized individuals. **(EISSG Control Reference: IA-6)**

10.8.6 **Cryptographic Module Authentication:** HHS Information systems shall use mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal/state laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication. **(EISSG Control Reference: IA-7)**

10.8.7 **Identification and Authentication (Non-Organizational Users):** HHS information systems shall uniquely identify and authenticate non-HHS users (or processes acting on behalf of non-HHS users). **(EISSG Control Reference: IA-8)**

10.9 Incident Response Policy (IR)

HHS management shall (i) establish an operational incident handling capability for HHS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) tracks, documents, and reports incidents to appropriate HHS and HHS officials and/or authorities.

Incident Response Policy Statements

The following incident response policy statements are required to satisfy the incident response policy.

10.9.1 **Incident Response Training:** HHS management shall train personnel in their incident response roles and responsibilities with respect to HHS information resources. **(EISSG Control Reference: IR-2)**

10.9.2 **Incident Response Testing:** HHS management shall test and/or exercise the incident response capability for HHS. **(EISSG Control Reference: IR-3)**

10.9.3 **Incident Handling:** HHS management shall implement an incident handling capability for HHS. Incident handling shall include coordinating activities with contingency planning, incorporating lessons learned into incident response procedures, training, and

testing/exercises, and implementing the resulting changes accordingly. **(EISSG Control Reference: IR-4)**

10.9.4 Incident Monitoring: HHS management shall track and document security incidents for HHS. **(EISSG Control Reference: IR-5)**

10.9.5 Incident Reporting: HHS management shall require personnel to report suspected security incidents to the HHS incident response capability. HHS management shall report security incident information to designated authorities. **(EISSG Control Reference: IR-6)**

10.9.6 Incident Response Assistance: HHS management shall provide an incident response support resource, integral to the HHS incident response capability. **(EISSG Control Reference: IR-7)**

10.9.7 Incident Response Plan: HHS management shall develop, distribute, coordinate, review, and communicate an incident response plan for HHS. **(EISSG Control Reference: IR-8)**

10.9.8 Information Spillage Response: HHS management shall ensure personnel follow HHS Incident Response procedures for information spills **(EISSG Control Reference: IR-9)**

10.10 Maintenance Policy (MA)

HHS management shall ensure that (i) periodic and timely maintenance on HHS information systems occur; and (ii) effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance are in place.

Maintenance Policy Statements

The following maintenance policy statements are required to satisfy the maintenance policy.

10.10.1 Controlled Maintenance: HHS management shall schedule, perform, document, and review the records of maintenance and repairs on information system components. This requires that a designated official explicitly approve the removal of a component, sanitize equipment, and check all potentially impacted security controls following maintenance or repair actions. **(EISSG Control Reference: MA-2)**

10.10.2 Maintenance Tools: HHS management shall approve, control, monitor the use of, and maintain on an ongoing basis, the maintenance tools for HHS. **(EISSG Control Reference: MA-3)**

10.10.3 Non-Local Maintenance: HHS management shall authorize, monitor, and control non-local maintenance and diagnostic activities for HHS. **(EISSG Control Reference: MA-4)**

10.10.4 Maintenance Personnel: HHS management shall establish a process for maintenance personnel authorization and maintain a current list of authorized maintenance organizations or personnel. **(EISSG Control Reference: MA-5)**

10.10.5 Timely Maintenance: HHS management shall obtain timely maintenance support and/or spare parts for HHS information system components. **(EISSG Control Reference: MA-6)**

10.11 Media Protection Policy (MP)

HHS management shall (i) ensure the protection of HHS digital and non-digital information system media; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Media Protection Policy Statements

The following media protection policy statements are required to satisfy the media protection policy.

10.11.1 Media Protection Policy and Procedures: HHS management shall ensure development, documentation and dissemination to applicable personnel. **(EISSG Control Reference: MP-1)**

10.11.2 Media Access: HHS management shall restrict access to HHS media (digital and non-digital) to authorized individuals. **(EISSG Control Reference: MP-2)**

10.11.3 Media Marking: HHS management shall mark removable media and output for HHS components to indicate the distribution limitations, handling caveats, and applicable security markings (if any) of the information. **(EISSG Control Reference: MP-3)**

10.11.4 Media Storage: HHS management shall physically control and securely store media within controlled areas using safeguards prescribed for the classification of the data contained on the media. **(EISSG Control Reference: MP-4)**

10.11.5 Media Transport: HHS management shall protect HHS media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. **(EISSG Control Reference: MP-5)**

10.11.6 Media Sanitation: HHS management shall sanitize HHS information system media both digital and non-digital prior to disposal, release out of HHS control, or release for reuse. **(EISSG Control Reference: MP-6)**

10.11.7 Media Use: HHS prohibits the use of portable storage devices in HHS information systems when such devices have no identifiable owner. **(EISSG Control Reference: MP-7)**

10.12 Physical and Environmental Protection Policy (PE)

HHS management shall coordinate with Texas Facilities Commission (TFC) and/or other owning facility management organizations to (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Physical and Environmental Protection Policy Statements

The following physical and environmental policy statements are required to satisfy the physical and environmental policy.

10.12.1 Physical Access Authorizations: HHS management shall develop and keep current a list of personnel with authorized access to the facility where HHS information resources components reside. **(EISSG Control Reference: PE-2)**

10.12.2 Physical Access Control: HHS management shall enforce physical access authorizations for all physical access points to the facility where HHS information resources components reside. **(EISSG Control Reference: PE-3)**

10.12.3 Access Control for Transmission Medium: HHS management shall control physical access to HHS information resources component distribution and transmission lines within organizational facilities. **(EISSG Control Reference: PE-4)**

10.12.4 Access Control for Output Devices: HHS management shall control physical access to HHS information resources component output devices to prevent unauthorized individuals from obtaining the output. **(EISSG Control Reference: PE-5)**

10.12.5 Monitoring Physical Access: HHS management shall ensure monitoring of physical access to the HHS information system to detect and respond to physical security incidents. **(EISSG Control Reference: PE-6)**

10.12.6 Visitor Access Records: HHS management shall maintain visitor access records to the facility where the HHS components reside. **(EISSG Control Reference: PE-8)**

10.12.7 Power Equipment and Power Cabling: HHS management shall protect power equipment and power cabling for HHS components from damage and destruction. **(EISSG Control Reference: PE-9)**

10.12.8 Emergency Shutoff: HHS management shall provide the capability of shutting off power to HHS information resources components in emergency situations. **(EISSG Control Reference: PE-10)**

10.12.9 Emergency Power: HHS management shall provide a short-term uninterruptible power supply to facilitate an orderly shutdown of HHS components in the event of a primary power source loss. **(EISSG Control Reference: PE-11)**

10.12.10 Emergency Lighting: HHS management shall employ and maintain automatic emergency lighting for HHS components that activates in the event of a power outage or disruption. **(EISSG Control Reference: PE-12)**

10.12.11 Fire Protection: HHS management shall employ and maintain fire suppression and detection devices/systems for HHS components that are supported by an independent energy source. **(EISSG Control Reference: PE-13)**

10.12.12 Temperature and Humidity Controls: HHS management shall maintain temperature and humidity levels in the facility where HHS components reside within acceptable vendor-recommended levels. **(EISSG Control Reference: PE-14)**

10.12.13 Water Damage Protection: HHS management shall protect HHS information resources components from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. **(EISSG Control Reference: PE-15)**

10.12.14 Delivery and Removal: HHS management shall authorize, monitor, and control the movement of HHS components entering and exiting the facility. **(EISSG Control Reference: PE-16)**

10.12.15 Alternate Work Site: HHS management shall employ appropriate security controls at alternate work sites. **(EISSG Control Reference: PE-17)**

10.13 Planning Policy (PL)

HHS management shall ensure the development, documentation, periodic update, and implementation of security plans for HHS.

Planning Policy Statements

The following planning policy statements are required to satisfy the planning policy.

10.13.1 System Security Plan: HHS management shall develop a consistent security plan for HHS information systems. **(EISSG Control Reference: PL-2)**

10.13.2 Rules of Behavior: HHS management shall establish and make readily available to all HHS users the HHS rules that describe their responsibilities and expected behavior with regard to information, the information system, and network use. **(EISSG Control Reference: PL-4)**

10.13.3 Information Security Architecture: HHS management shall ensure the development of information security architecture for the information system. **(EISSG Control Reference: PL-8)**

10.14 Personnel Security Policy (PS)

HHS management shall work with HHS human resources to (i) ensure that individuals occupying positions of responsibility within HHS (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that HHS information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with HHS security policies and procedures.

Personnel Security Policy Statements

The following personnel security policy statements are required to satisfy the personnel security policy.

10.14.1 Position Risk Designation: HHS management shall assign a risk designation to all positions. **(EISSG Control Reference: PS-2)**

10.14.2 Personnel Screening: HHS management shall screen individuals, according to the HHS Human Resources (HR) Manual requirements. **(EISSG Control Reference: PS-3)**

10.14.3 Personnel Termination: HHS management shall revoke physical access immediately following employee termination and system access prior to or during the employee termination process. **(EISSG Control Reference: PS-4)**

10.14.4 Personnel Transfer: HHS management shall periodically review the logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within HHS organization. **(EISSG Control Reference: PS-5)**

10.14.5 Access Agreements: HHS management shall ensure that individuals requiring access to HHS information resources information and HHS components sign appropriate access agreements prior to being granted access. **(EISSG Control Reference: PS-6)**

10.14.6 Third Party Personnel Security: HHS management shall establish personnel security requirements, document personnel security requirements, and monitor provider compliance. **(EISSG Control Reference: PS-7)**

10.14.7 Personnel Sanctions: HHS management shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures. **(EISSG Control Reference: PS-8)**

10.15 Risk Assessment Policy (RA)

HHS management shall assess the risks to HHS information resources resulting from the operation of HHS information systems and the associated processing, storage, or transmission of HHS information. Risk assessments shall be risked-based and include all HHS information and information resources whether internal or external.

Risk Assessment Policy Statements

The following risk assessment policy statements are required to satisfy the risk assessment policy.

10.15.1 Security Categorization: HHS management shall categorize information and HHS information resources components in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, and guidelines. **(EISSG Control Reference: RA-2)**

10.15.2 Risk Assessment: HHS management shall conduct an assessment of risk of the HHS information systems and the information it processes, stores, or transmits. **(EISSG Control Reference: RA-3)**

10.15.3 Vulnerability Scanning: HHS management shall scan for vulnerabilities in HHS information systems regularly. **(EISSG Control Reference: RA-5)**

10.16 System and Services Acquisition Policy (SA)

HHS management shall (i) ensure sufficient allocation of resources to adequately protect HHS information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from HHS.

System and Services Acquisition Policy Statements

The following system and services acquisition policy statements are required to satisfy the system and services acquisition policy.

10.16.1 Allocation of Resources: HHS management shall include a determination of information security requirements for the HHS components in mission/business process planning. **(EISSG Control Reference: SA-2)**

10.16.2 System Development Life Cycle (SDLC): HHS management shall manage the HHS components using a system development life cycle methodology and security shall be included in all phases of the life cycle (Secure-SDLC aka S-SDLC). **(EISSG Control Reference: SA-3)**

10.16.3 Acquisition Process: HHS management shall include security functional requirements/specifications, explicitly or by reference, in HHS component acquisition contracts based on an assessment of risk and in accordance with applicable federal/state laws, executive orders, directives, policies, regulations, and standards. **(EISSG Control Reference: SA-4)**

10.16.4 Information System Documentation: HHS management shall obtain, and make available to authorized personnel, administrator documentation for the information system. **(EISSG Control Reference: SA-5)**

10.16.5 Security Engineering Principles: HHS management shall apply information system security engineering principles in the specification, design, development, implementation, and modification of the HHS information system networking, operating system, application, and other software components including database. **(EISSG Control Reference: SA-8)**

10.16.6 External Information System Services: HHS management shall require that providers of external information system services comply with organizational information security requirements. **(EISSG Control Reference: SA-9)**

10.16.7 Developer Configuration Management: HHS management shall require that HHS developers/integrators perform configuration management. **(EISSG Control Reference: SA-10)**

10.16.8 Developer Security Testing and Evaluation: HHS management shall require that HHS component developers/integrators create and implement a security test and evaluation plan in consultation with information security personnel. **(EISSG Control Reference: SA-11)**

10.16.9 Unsupported System Components: HHS management shall ensure information systems are replaced when support for the components is no longer available. **(EISSG Control Reference: SA-22)**

10.17 System and Communication Protection Policy (SC)

HHS management shall (i) ensure the monitoring, control, and protection of HHS communications (information transmitted or received by HHS information systems) at the external and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within HHS information systems.

System and Communication Protection Policy Statements

The following system and communication protection policy statements are required to satisfy the system and communication protection policy.

10.17.1 Application Partitioning: HHS information systems shall separate user functionality (including user interface services) from management functionality. **(EISSG Control Reference: SC-2)**

10.17.2 Information in Shared Resources: HHS information systems shall prevent unauthorized and unintended information transfer via shared system resources. **(EISSG Control Reference: SC-4)**

10.17.3 Denial of Service Protection: HHS information systems shall protect against or limit the effects of distributed denial of service (DDoS) attacks. **(EISSG Control Reference: SC-5)**

10.17.4 Resource Availability: HHS management shall protect the availability of resources by allocating resources by priority. **(EISSG Control Reference: SC-6**

10.17.5 Boundary Protection: HHS information systems shall monitor and control communications at the external boundary of HHS and at key internal boundaries within the system. **(EISSG Control Reference: SC-7)**

10.17.6 Transmission Confidentiality and Integrity: HHS information systems shall protect the confidentiality and integrity of transmitted information. **(EISSG Control Reference: SC-8)**

10.17.7 Network Disconnect: HHS information systems shall terminate the network connection associated with a communications session at the end of the session or when it has reached the limit of inactivity permitted. **(EISSG Control Reference: SC-10)**

10.17.8 Cryptographic Key Establishment and Management: HHS information systems, if applicable, shall establish and manage cryptographic keys for required cryptography employed within HHS. **(EISSG Control Reference: SC-12)**

10.17.9 Cryptographic Protection: HHS shall employ cryptographic protection mechanism in accordance with applicable federal and state laws, executive orders, directives, policies, regulations and standards. **(EISSG Control Reference: SC-13)**

10.17.9.1 Encryption on device: Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management shall be based on documented state agency risk management decisions.

10.17.9.2 Data at rest: Any end user devices including portable devices and desktops containing restricted or confidential information shall be encrypted. Also, any confidential data stored in the cloud shall be encrypted at rest.

10.17.9.3 Data in motion: Any confidential data transmitted over the internet or untrusted network paths shall be encrypted.

10.17.10 Collaborative Computing Devices: HHS management shall prohibit remote activation of collaborative computing devices on HHS information systems that are not explicitly approved by the agency. **(EISSG Control Reference: SC-15)**

10.17.11 Public Key Infrastructure Certificates: HHS management, if applicable, shall issue or obtain public key certificates under an appropriate certificate policy from an approved service provider. **(EISSG Control Reference: SC-17)**

10.17.12 Mobile Code: HHS management shall define acceptable and unacceptable mobile code and mobile code technologies. **(EISSG Control Reference: SC-18)**

10.17.13 Voice over Internet Protocol (VoIP): HHS management shall establish usage restrictions and implementation guidance for VoIP technologies. **(EISSG Control Reference: SC-19)**

10.17.14 Secure Name/Address Resolution Service (Authoritative Source): HHS information systems, if applicable, shall provide additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. **(EISSG Control Reference: SC-20)**

10.17.15 Secure Name/Address Resolution Service (Recursive or Caching Resolver): HHS information systems, if applicable, shall perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems. **(EISSG Control Reference: SC-21)**

10.17.16 Architecture and Provisions for Name/Address Resolution Service: HHS information systems, if applicable, shall provide name/address resolution service that are fault-tolerant and shall implement internal/external role separation. **(EISSG Control Reference: SC-22)**

10.17.17 Session Authenticity: HHS information systems shall provide mechanisms to protect the authenticity of communications sessions. **(EISSG Control Reference: SC-23)**

10.17.18 Protection of Information at Rest: HHS management shall protect the confidentiality and integrity of information at rest. **(EISSG Control Reference: SC-28)**

10.17.19 Information System Partitioning: HHS management shall ensure information systems are partitioned for physical separation of components. **(EISSG Control Reference: SC-32)**

10.17.20 Process Isolation: HHS information systems, if applicable, shall maintain a separate execution domain for each executing process. **(EISSG Control Reference: SC-39)**

10.18 System and Information Integrity Policy (SI)

HHS management shall ensure (i) the identification, reporting, and the correction of information system flaws in a timely manner; (ii) protection from malicious code at appropriate locations within HHS information systems; and (iii) the monitoring of information system security alerts and advisories, and execution of appropriate actions.

System and Information Integrity Policy Statements

The following system and information integrity policy statements are required to satisfy the system and information integrity policy.

10.18.1 Flaw Remediation: HHS management shall manage the remediation of flaws. **(EISSG Control Reference: SI-2)**

10.18.2 Malicious Code Protection: HHS management shall manage the protection of HHS from malicious code. **(EISSG Control Reference: SI-3)**

10.18.3 Information System Monitoring: HHS management shall monitor the HHS information system for malicious activity. **(EISSG Control Reference: SI-4)**

10.18.4 Security Alerts, Advisories and Directives: HHS management shall manage security alerts, advisories, and directives. **(EISSG Control Reference: SI-5)**

10.18.5 Security Function Verification: HHS management shall verify security functions. **(EISSG Control Reference: SI-6)**

10.18.6 **Software, Firmware and Information Integrity:** HHS management shall detect unauthorized changes to HHS information systems software, firmware and information**. (EISSG Control Reference: SI-7)**

10.18.7 **Spam Protection:** HHS management shall ensure the protection of HHS from unsolicited messages. **(EISSG Control Reference: SI-8)**

10.18.8 **Information Input Validation:** HHS information systems shall check the validity of information inputs. **(EISSG Control Reference: SI-10)**

10.18.9 **Error Handling:** HHS information systems shall manage error handling. **(EISSG Control Reference: SI-11)**

10.18.10 **Information Handling and Retention:** HHS management shall manage information output handling and retention within the information system and information output from the system in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, and operational requirements. **(EISSG Control Reference: SI-12)**

10.18.11 **Memory Protection:** HHS management shall employ security safeguards to protect the information systems memory from unauthorized code execution. **(EISSG Control Reference: SI-16)**

11. POLICY EXCEPTIONS

Exceptions to information security requirements or controls may be issued, but must be justified, documented, communicated, and approved as part of the risk assessment process. Agency information owners are responsible to justify, document, and be accountable for exceptions to security controls. The agency information owner shall coordinate exceptions to security controls with the agency Information Security Officer and participate in risk assessments.

Per TAC 202, Rule 202.25, Managing Security Risks, approval of the security risk acceptance, transference, or mitigation decisions shall be the responsibility of:

a) The Information Security Officer or his or her designee(s), in coordination with the information owner, for systems identified with Low or Moderate residual risk.
b) The state agency head for all systems identified with a residual High risk.

12. INQUIRIES

Inquiries regarding the content in this EIS-Policy should be directed to the Enterprise Information Security (EIS) Office at infosecurity@hhsc.state.tx.us